(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 740 291**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **95 12351**

(51) Int Cl⁶ : H 04 Q 7/32, H 04 L 9/32, H 04 B 7/26

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 20.10.95.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 25.04.97 Bulletin 97/17.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *SOCIETE D'APPLICATIONS GENERALES D'ELECTRICITE ET DE MECANIQUE SAGEM SOCIETE ANONYME* — FR.

(72) **Inventeur(s)** : SARRADIN JEAN LOUIS.

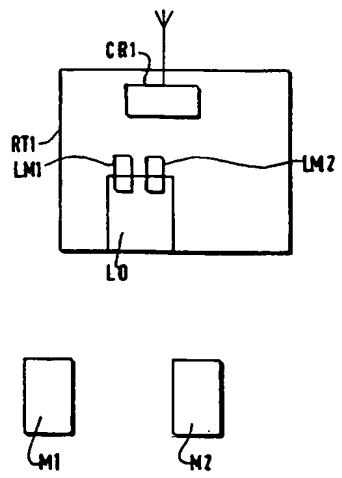
(73) **Titulaire(s)** :

(74) **Mandataire** : CABINET BLOCH.

(54) RADIOTELEPHONE A DOUBLE FONCTION, NOTAMMENT DE TRANSACTION FINANCIERE ET PROCEDE D'ETABLISSEMENT D'UNE COMMUNICATION ENTRE LE RADIOTELEPHONE ET LE RESEAU RADIOTELEPHONIQUE.

(57) Le radiotéléphone (RT1) comprend un circuit radio (CR1), un logement (LO) pour recevoir un premier module (M1) portant un microcircuit, une première interface de lecture/écriture (LM1) pour faire communiquer le microcircuit avec le circuit radio, une seconde interface de lecture/écriture (LM2) pour lire et écrire des données dans un second module portant un microcircuit (M2).

Les première et seconde interfaces (LM1, LM2) sont disposées dans le logement (LO) dans lequel peuvent être insérées successivement les premier et second modules. Grâce à l'invention, une carte bancaire peut être utilisée avec un radiotéléphone.



FR 2 740 291 - A1

RADIOTELEPHONE A DOUBLE FONCTION, NOTAMMENT DE TRANSACTION FINANCIERE ET PROCEDE D'ETABLISSEMENT D'UNE COMMUNICATION ENTRE LE RADIOTELEPHONE ET LE RESEAU RADIOTELEPHONIQUE

La présente invention concerne un radiotéléphone pour établir et recevoir des communications via un réseau radiotéléphonique.

Un radiotéléphone, tel qu'actuellement disponible, par exemple pour accéder au réseau GSM, utilise un module d'identité d'abonné, dit module SIM, pour authentifier et autoriser une communication préalablement à son établissement.

Une fois la communication établie, de nouveaux services nécessitant par exemple un paiement par carte bancaire ne sont actuellement pas accessibles à l'usager du radiotéléphone en raison de l'impossibilité d'utiliser une carte bancaire avec le radiotéléphone. D'autres services utilisant une carte applicative spécifique sont de même exclus d'accès par un radiotéléphone.

La présente invention vise à remédier aux inconvénients précités en proposant un radiotéléphone à double fonction, qui permet l'utilisation d'une carte telle qu'une carte de transaction financière, telle que carte bancaire.

A cet effet, l'invention concerne tout d'abord un radiotéléphone comprenant un circuit radio, un logement pour recevoir un premier module portant un microcircuit, une première interface de lecture/écriture pour faire communiquer le microcircuit avec le circuit radio, caractérisé par le fait qu'il comprend une seconde interface de lecture/écriture pour lire et écrire des données dans un second module portant un microcircuit.

De façon intéressante, les première et seconde interfaces sont disposées dans le logement dans lequel peuvent être insérés successivement les premier et second modules.

Dans une autre forme de réalisation, il est prévu un second logement pour recevoir le second module, ladite seconde interface étant disposée dans le second logement.

Dans une variante de réalisation, la seconde interface est disposée dans un second logement ménagé dans un terminal externe relié au circuit radio du radiotéléphone par une liaison filaire.

De façon préférée, ladite seconde interface est agencée pour coopérer avec une carte bancaire.

La demanderesse entend également revendiquer un radiotéléphone caractérisé par le fait qu'il comprend un circuit radio, un logement de réception d'un module portant un microcircuit de communication radio et de transaction financière et une interface de lecture/écriture pour faire communiquer le microcircuit avec le circuit radio et lire et écrire des données financières dans le module.

L'invention concerne également un procédé pour établir une communication de données entre un radiotéléphone et un réseau radiotéléphonique, caractérisé par le fait qu'il comprend après la mise sous tension du radiotéléphone les étapes suivantes:

- détecter la présence d'un module d'identité d'abonné,
- authentifier l'abonné et établir une communication entre le radiotéléphone et un équipement distant via le réseau radiotéléphonique,
- détecter la présence d'un second module portant un microcircuit, et
- échanger des données entre le microcircuit du second module détecté et l'équipement distant.

L'invention sera mieux comprise à l'aide de la description suivante, en référence au dessin annexé, sur lequel :

- la figure 1 représente un radiotéléphone et une station de base d'un réseau radiotéléphonique, selon la technique antérieure;
- la figure 2 est un algorithme d'authentification selon la technique antérieure;
- la figure 3 est une première réalisation d'un radiotéléphone selon l'invention;
- la figure 4 est un algorithme schématisant le fonctionnement du radiotéléphone de la figure 3;
- la figure 5 est une seconde réalisation d'un radiotéléphone selon l'invention et
- la figure 6 est une troisième réalisation d'un radiotéléphone selon l'invention.

En référence à la figure 1, une station mobile connue, telle qu'un radiotéléphone portatif RT, est utilisable pour émettre et recevoir des communications téléphoniques via un réseau radiotéléphonique dont une station de base SB est représentée à la figure 1. La station de base SB dessert une zone géographique dans laquelle se trouve le radiotéléphone RT. Le réseau radiotéléphonique est par exemple le réseau GSM (Global System for Mobile communications).

Afin d'empêcher un usage frauduleux du radiotéléphone RT, un module d'identité d'abonné M, dit module SIM (Subscriber Identity Module), est utilisé pour authentifier l'usager préalablement à tout établissement d'une communication.

Le module M est amovible et se présente sous la forme d'une carte au format ISO sur laquelle est implanté un microcircuit. Le module M est insérable dans un logement incorporé au radiotéléphone RT.

Le module SIM peut être enfichable, de taille réduite.

Un module M communique avec un circuit radio CR du radiotéléphone RT.

Le module M contient un numéro international d'abonné IMSI (International Mobile Subscriber Identity), une clé d'authentification individuelle Ki et un algorithme d'authentification.

En référence à la figure 2, l'algorithme d'authentification comprend cinq étapes E1 à E5 préalables à l'établissement d'une communication. Les étapes E1 et E3 sont réalisées dans le module M du radiotéléphone RT. Les étapes E2, E4 et E5 sont réalisées dans un équipement de gestion du réseau RT.

A l'étape E1, l'usager du radiotéléphone RT s'identifie dans le réseau. Le numéro IMSI est émis vers la station de base SB desservant la zone géographique dans laquelle se trouve le radiotéléphone RT.

Le numéro IMSI est reçu par le réseau. A l'étape E2, le réseau émet un nombre aléatoire RAND vers le radiotéléphone RT en réponse au numéro IMSI.

A l'étape E3 effectuée dans le radiotéléphone RT, l'algorithme d'authentification calcule une signature de réponse SRES1 en fonction du nombre aléatoire reçu RAND et de la clé d'identification Ki.

De même, à l'étape E4, le réseau calcule une signature de réponse SRES2 en fonction du nombre aléatoire RAND et de la clé Ki du radiotéléphone RT.

Le radiotéléphone RT émet la signature SRES1 vers le réseau. Les signatures SRES1 et SRES2 sont alors comparées à l'étape E5 et une communication est établie si les signatures SRES1 et SRES2 sont égales.

En variante, un numéro d'identité personnelle PIN (Personal Identification Number) est mémorisé dans le module

M. L'usager doit alors saisir son numéro d'identité personnelle au clavier à chaque fois qu'il insère le module M dans le logement qui lui est réservé dans le radiotéléphone RT, ou à chaque mise en service de ce dernier. Le numéro saisi est comparé au numéro mémorisé et si les deux numéros sont égaux l'utilisation du radiotéléphone est autorisée.

En référence à la figure 3, un radiotéléphone RT1 selon une première forme de réalisation de l'invention comprend un logement LO pour recevoir un module SIM M1 se présentant sous la forme d'une carte au format ISO et portant un microcircuit.

Le logement LO a des dimensions adaptées à celles du module SIM M1. Une première interface de lecture/écriture LM1 équipe le logement LO pour lire des données mémorisées dans le microcircuit du module SIM M1 et les transmettre au circuit radio CR1 du radiotéléphone RT1. Les données mémorisées sont notamment le numéro IMSI et la clé Ki. L'interface LM1 écrit des données dans le microcircuit du module SIM M1, qui sont reçues via le circuit radio CR1 du radiotéléphone RT1. Les données reçues sont notamment le nombre RAND.

Le logement LO comprend une seconde interface de lecture/écriture LM2. L'interface LM2 lit et écrit des données dans un microcircuit d'un second module M2 se présentant sous la forme d'une carte au format ISO et portant un microcircuit. Le second module M2 est par exemple une carte bancaire, ou une carte dédiée à une application spécifique telle qu'affiliation à une centrale d'achat ou à une association.

Le microcircuit du second module M2 est situé à un emplacement différent de celui du module SIM M1. Ainsi, l'interface LM1 reconnaît le module SIM M1 lorsque ce dernier est inséré dans le logement LO en détectant le

microcircuit du module M1. De même, l'interface LM2 reconnaît le second module M2 lorsqu'il est inséré dans le logement LO, en détectant le microcircuit du module M2.

Le fonctionnement du radiotéléphone RT1 est schématisé à la figure 4 par cinq étapes E11 à E15.

L'étape E11 est la mise sous tension du radiotéléphone RT1 suivie d'une initialisation pour localiser et signaler le radiotéléphone RT1 dans le réseau radiotéléphonique.

L'étape E12 est la détection du module SIM M1 dans le logement Lo. Si le module SIM M1 n'est pas détecté, aucune communication n'est établie et le radiotéléphone RT1 demeure à l'état de veille.

Lorsque le module M1 est détecté, l'étape E13 d'authentification et d'établissement d'une communication est réalisée. L'étape E13 est analogue à la succession des étapes E1 à E5 précédemment décrites.

Si la communication établie est une communication "classique" de parole entre l'usager du radiotéléphone RT1 et un autre usager téléphonique, le fonctionnement du radiotéléphone RT1 est analogue à celui du radiotéléphone connu RT.

Si la communication est établie vers un serveur spécifique correspondant à l'utilisation du module M2, l'usager du radiotéléphone RT1 retire alors le module M1 du logement LO et insère le module M2 dans le logement LO.

A l'étape E14, le module M2 est détecté par la seconde interface LM2 et des données sont échangées entre le module M2 et le serveur spécifique. La nature et le format des données échangées ainsi que le protocole d'échange dépendent de l'application qui est par exemple un paiement, un vote ou la participation à un jeu. La communication de données entre le radiotéléphone RT1 et le serveur est réalisée à l'étape E15.

Selon une seconde réalisation de l'invention représentée à la figure 5, un radiotéléphone RT2 comprend un premier logement LO1 équipé de la première interface de lecture/écriture LM1. Le module SIM M1 est insérable dans le logement LO1 comme précédemment décrit.

Le radiotéléphone RT2 comprend un second logement LO2 équipé de la seconde interface de lecture/écriture LM2. Le second module M2 est insérable dans le logement LO2.

Le fonctionnement du radiotéléphone RT2 est analogue à celui du radiotéléphone RT1 décrit en référence à la figure 4. Il n'est pas nécessaire de retirer le module M1 pour insérer le module M2. Les deux modules M1 et M2 peuvent être présents simultanément dans le radiotéléphone RT2.

En variante, le radiotéléphone RT2 comprend un module SIM enfichable de taille plus réduite qu'une carte au format ISO. Le radiotéléphone RT2 comprend le logement LO2 pour insérer le second module M2 qui est présent simultanément avec le module SIM enfichable dans le radiotéléphone RT2.

En référence à la figure 6, un radiotéléphone RT3 selon une troisième réalisation de l'invention comprend un logement LO3 pour recevoir le module SIM M1 et une interface de lecture/écriture LM3 pour lire et écrire des données dans le microcircuit du module SIM M1. L'interface LM3 communique avec le circuit radio CR3 du radiotéléphone RT3.

Un terminal externe TE est relié par une liaison filaire LF au radiotéléphone RT3. Le terminal externe TE comprend un logement LO4 pour recevoir le module M2. Une interface de lecture/écriture LM4 lit et écrit des données dans le microcircuit du module M2. L'interface LM4 est reliée au circuit radio CR3 du radiotéléphone RT3 par la liaison filaire LF.

Le fonctionnement du radiotéléphone RT3 associé au terminal externe TE est analogue à celui décrit en référence à la figure 4.

REVENDICATIONS

1 - Radiotéléphone (RT1, RT2, RT3) comprenant un circuit radio (CR1, CR2, CR3), un logement (LO, LO1, LO3) pour recevoir un premier module (M1) portant un microcircuit, une première interface de lecture/écriture (LM1, LM3) pour faire communiquer le microcircuit avec le circuit radio, caractérisé par le fait qu'il comprend une seconde interface de lecture/écriture (LM2) pour lire et écrire des données dans un second module portant un microcircuit (M2).

2 - Radiotéléphone (RT1) selon la revendication 1, dans lequel les première et seconde interfaces (LM1, LM2) sont disposées dans le logement (LO) dans lequel peuvent être insérés successivement les premier et second modules.

3 - Radiotéléphone (RT2) selon la revendication 1, comprenant un second logement (LO2) pour recevoir le second module, ladite seconde interface (LM2) étant disposée dans le second logement (LO2).

4 - Radiotéléphone (RT3) selon la revendication 1, dans lequel la seconde interface (LM4) est disposée dans un second logement (LO4) ménagé dans un terminal externe (TE) relié au circuit radio du radiotéléphone par une liaison filaire (LF).

5 - Radiotéléphone selon l'une des revendications 1 à 4, dans lequel ladite seconde interface (LM2, LM4) est agencée pour coopérer avec une carte de transaction financière.

6 - Radiotéléphone caractérisé par le fait qu 'il comprend un circuit radio, un logement de réception d'un module portant un microcircuit de communication radio et de transaction financière et une interface de lecture/écriture pour faire communiquer le microcircuit avec le circuit radio et lire et écrire des données financières dans le module.

7 - Procédé pour établir une communication de données entre un radiotéléphone et un réseau radiotéléphonique, caractérisé par le fait qu'il comprend après la mise sous tension du radiotéléphone les étapes suivantes:

- détecter la présence d'un module d'identité d'abonné,
- authentifier l'abonné et établir une communication entre le radiotéléphone et un équipement distant via le réseau radiotéléphonique,
- détecter la présence d'un second module portant un microcircuit, et
- échanger des données entre le microcircuit du second module détecté et l'équipement distant.

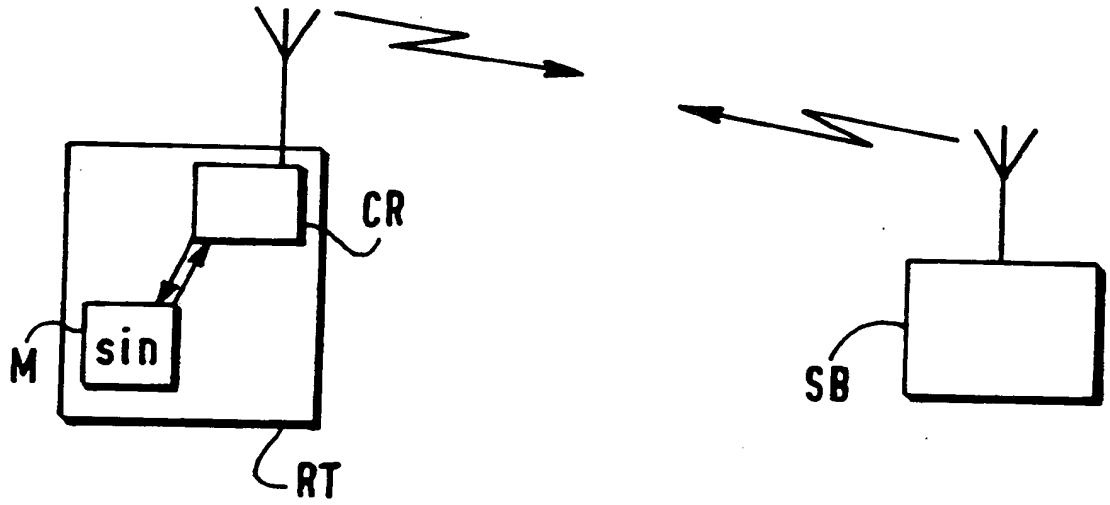


FIG.1

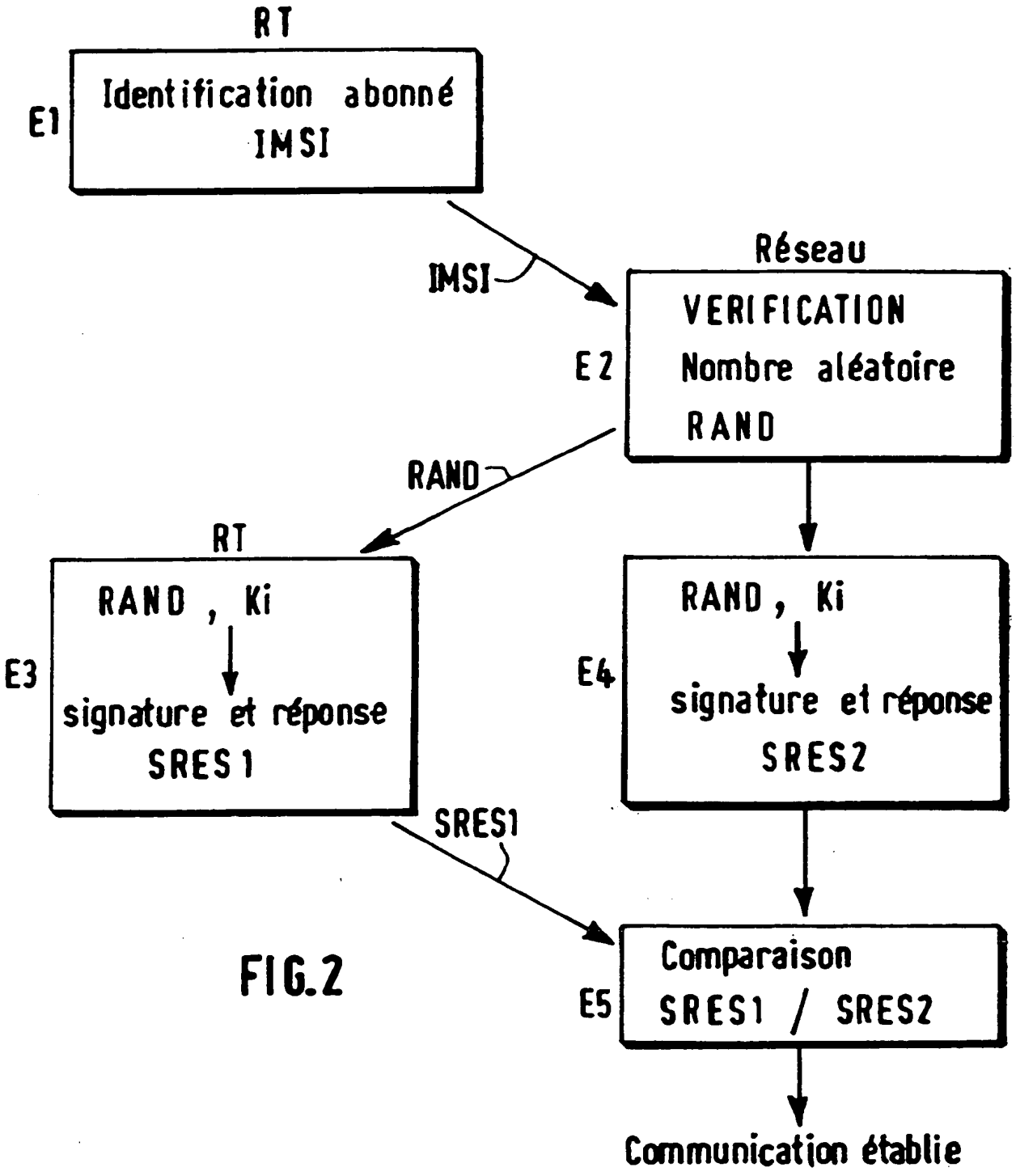
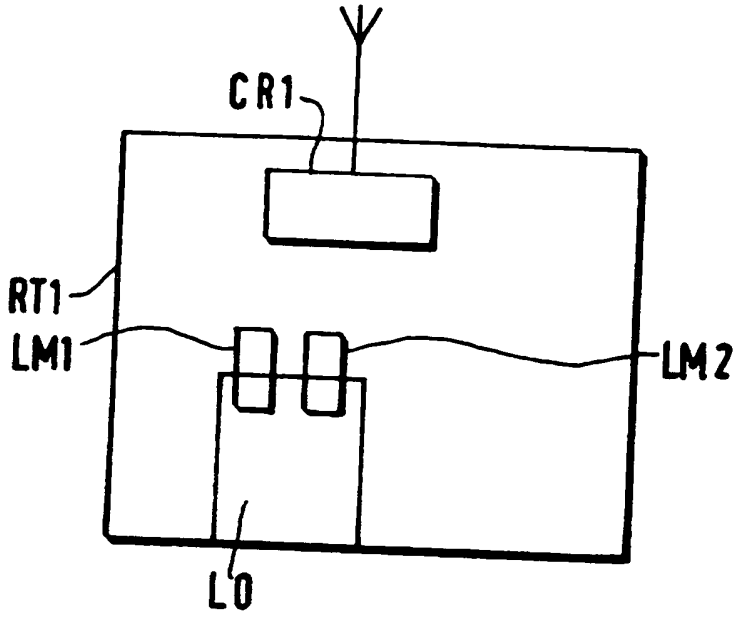


FIG.2



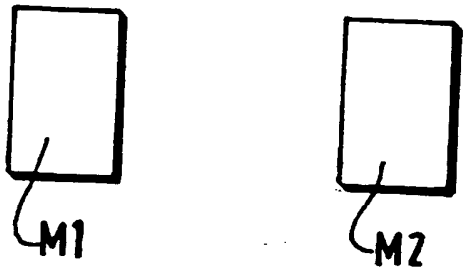


FIG.3

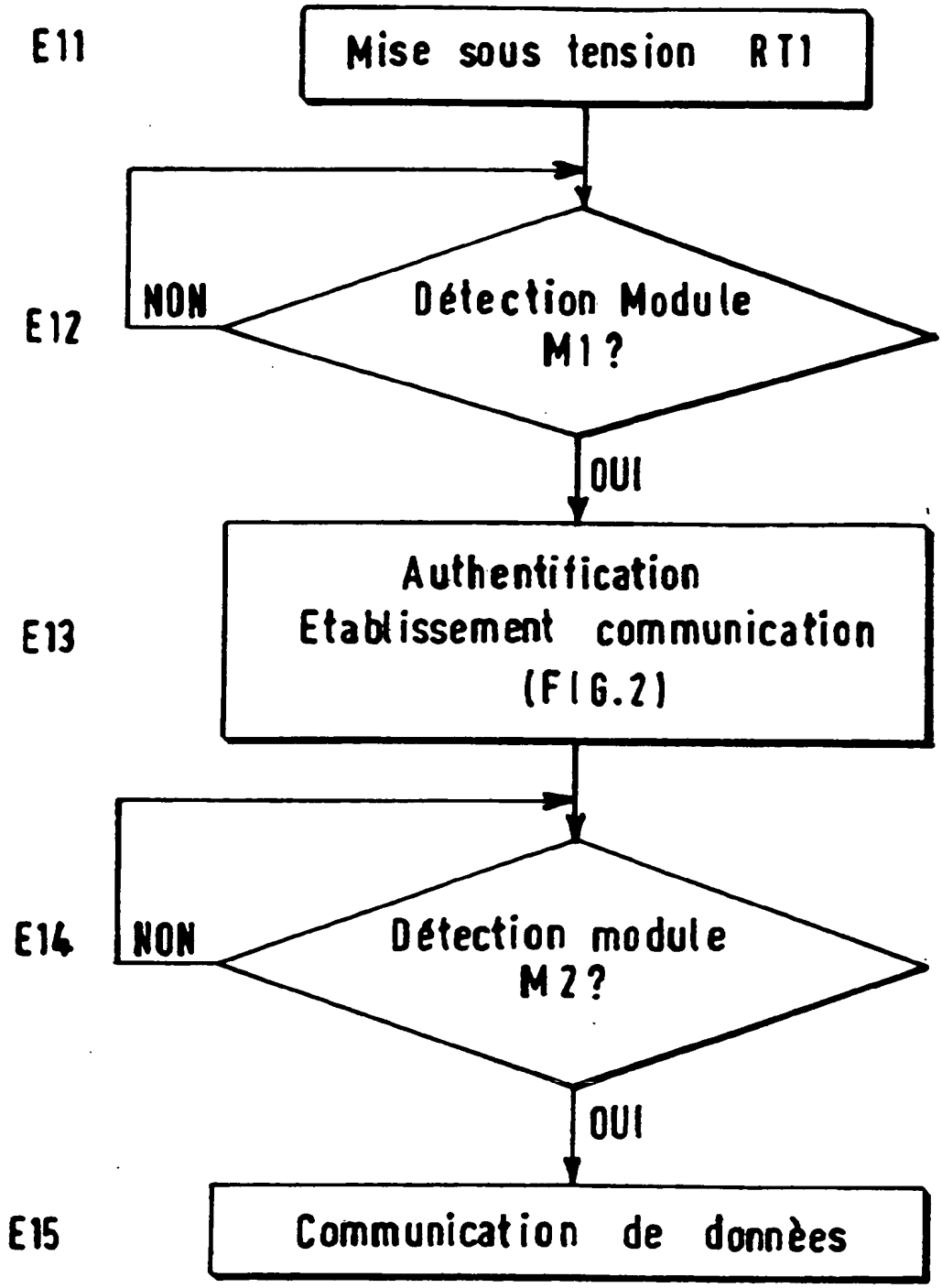


FIG.4

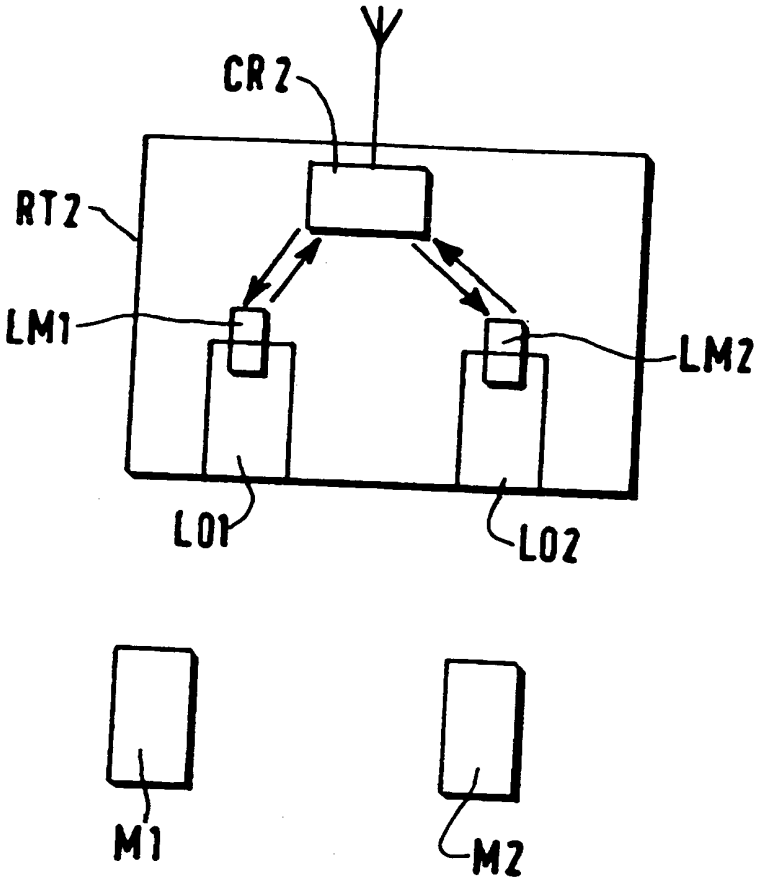


FIG.5

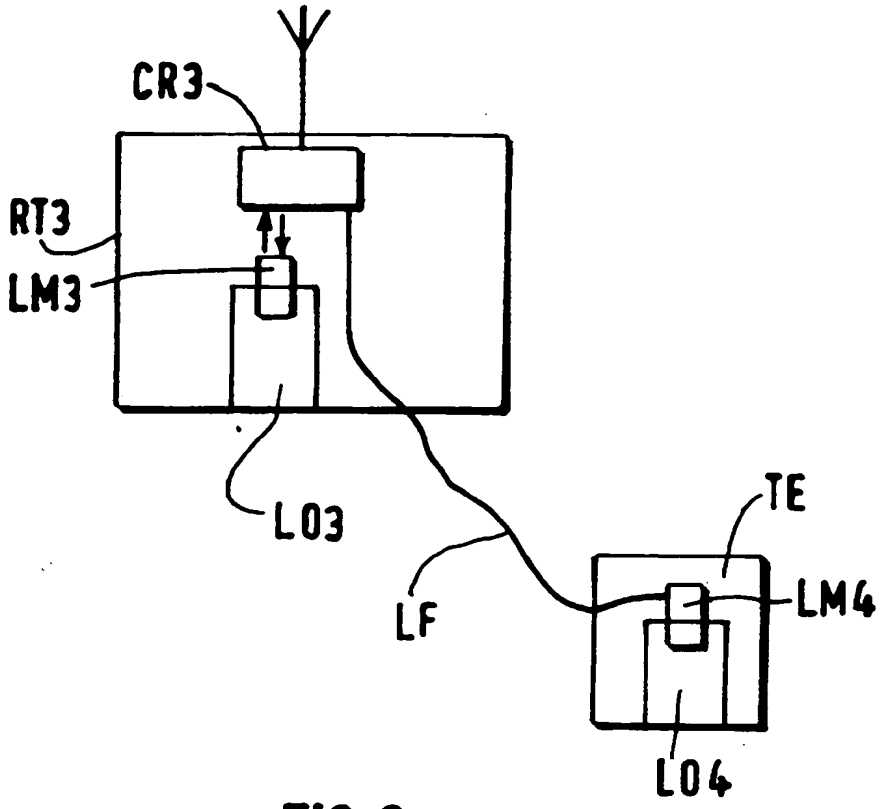


FIG. 6

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2740291
N° d'enregistrement national

FA 520445
FR 9512351

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	WO-A-94 11849 (VATANEN HARRI TAPANI) 26 Mai 1994	1,6,7
A	* page 6, ligne 17 - page 11, ligne 22; figures *	1-5
X	GB-A-2 269 512 (NOKIA MOBILE PHONES R & D ;NOKIA MOBILE PHONES LTD (FI)) 9 Février 1994	1-5
A	* revendications *	5-7
X	WO-A-94 30023 (CELLTRACE COMMUNICATIONS LIMIT ;MICHAELS WAYNE DAVID (GB); TIMSON) 22 Décembre 1994	6,7
A	* page 2, ligne 10 - ligne 27 * * page 6, ligne 5 - ligne 31 * * page 10, ligne 10 - ligne 28; figures *	1
A	EP-A-0 264 023 (HARRIS ARLENE J) 20 Avril 1988 * revendications 1-3,8-10 *	1-7
A	EP-A-0 589 757 (FRANCE TELECOM ;POSTE (FR)) 30 Mars 1994 * colonne 12, ligne 52 - colonne 15, ligne 3; revendications 1,8-10 *	1,6,7

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

H04Q

2

Date d'achèvement de la recherche: 18 Juillet 1996

Examinateur: Janyszek, J-M

EPO FORM 1503 03.82 (P04C13)

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant